**IN THE UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF VIRGINIA
Newport News Division**

SPACE SYSTEMS/LORAL, LLC	)	
	)	
Plaintiff,	)	4:17-cv-00025-RAJ-LRL
	)	
vs.	)	
	)	
ORBITAL ATK, INC.,	)	
	)	
Defendant.	)	
_____	)	

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION
TO DISMISS FOR FAILURE TO STATE A CLAIM
<u>UPON WHICH RELIEF MAY BE GRANTED</u>**

Bernard J. DiMuro, Esq. (VSB #187784)
Bill B. Ruhling, II, Esq. (VSB #45822)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, Virginia 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Emails: bdimuro@dimuro.com
        bruhling@dimuro.com

Rebecca R. Anzidei (VSB #46436)
Philip J. O'Beirne (VSB #71956)
**Stein Mitchell Cipollone Beato & Missner
LLP**
1100 Connecticut Avenue, NW Suite 1100
Washington, D.C. 20036
Telephone: (202) 737-7777
Facsimile: (202) 296-8312
Email: ranzidei@steinmitchell.com
        pobeirne@steinmitchell.com

Counsel for Defendant Orbital ATK, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

<u>**Cases**</u>

Statutes

Rules

Pursuant to Federal Rule of Civil Procedure 12(b)(6) and Local Rule 7(F)(1), Defendant Orbital ATK, Inc. ("Orbital ATK") respectfully submits this memorandum in support of its Motion to Dismiss for Failure to State a Claim Upon Which Relief May be Granted.

I. INTRODUCTION

Plaintiff Space Systems/Loral's ("SSL") Complaint is a meritless, tactically-motivated strike against Orbital ATK, a competitor. SSL's improper motive is evidenced by the weakness of its pleading and the timing of when it was filed. SSL's own allegations show:

- Orbital ATK *did not steal* SSL's business information; rather, *a government entity, NASA, provided an Orbital ATK employee* access to a shared server on which SSL's confidential information was stored, as part of that employee's legitimate work responsibilities on the Commercial Infrastructure for Robotic Assembly and Services (CIRAS) project;

- Orbital ATK told SSL that the employee who inappropriately accessed documents other than those relating to the CIRAS project was fired, that the information was not used, printed, copied or retained, and that Orbital ATK was cooperating fully with NASA;

- SSL's complaint is completely devoid of any allegation, or even inference, that the information accessed by Orbital ATK's former employee has been disclosed, used, or even referred to in any way since the access occurred last November;

- SSL is unable to articulate with anywhere near the requisite specificity (as opposed to boilerplate legal conclusions) that such information constituted protected trade secrets; and

- Not surprisingly, SSL has not pled any plausible facts that it has suffered — or is even likely to suffer — any actual harm as a result of what allegedly transpired.

For these reasons, SSL did not file suit against Orbital ATK when it learned of the foregoing through transparent communications from both NASA and Orbital ATK in December 2016. Instead, SSL waited *more than three months* to file the complaint – and only after *Orbital ATK* filed a lawsuit against the Defense Advanced Research Projects Agency ("DARPA") challenging the legality of the terms of a lucrative in-space satellite servicing

technology contract SSL obtained on a different project. Confirming that its suit is a baseless retaliation against Orbital ATK, at no point has SSL sought a temporary restraining order or preliminary injunction to protect its supposed trade secret information. SSL did not even serve Orbital ATK with the complaint until after Orbital ATK's counsel contacted counsel for SSL. Rather, SSL used this lawsuit as an opportunity to smear Orbital ATK in the press.[1]

Given the foregoing, it is no wonder that SSL's complaint fails to state a claim as a matter of law and should be dismissed. *First*, SSL's Computer Fraud and Abuse Act claim (Claim I) is barred by clear Eastern District of Virginia precedent that prevents claims against a party who accessed information that the Plaintiff itself provided and allowed to be stored on a third party's server. *Second*, this same claim fails because SSL failed to adequately plead "damage," which SSL was required to allege plausibly to state a CFAA claim. *Third*, SSL's general laundry list of categories of information falls far short of the level of specificity necessary to allege that the information supposedly accessed is entitled to trade secret protections. This is fatal to both SSL's federal Defend Trade Secrets Act claim (Claim II), as well as its state law Misappropriation of Trade Secrets/Virginia Uniform Trade Secrets Act claim (Claim III). *Fourth,* because the Orbital ATK employee was authorized to access NASA's NX server, SSL cannot state a claim for a violation of the Virginia Computer Crimes Act (Claim IV). *Finally*, both of SSL's state common law claims for conversion (Claim V) and unjust enrichment (Claim VI) are preempted by statute and must be dismissed.

---

[1] (http://spacenews.com/ssl-sues-orbital-atk-over-confidential-data-breach/, attached hereto as Ex. 1) "A court can take judicial notice of a newspaper article at the motion to dismiss stage when the article discusses the subject matter of the case." *Advanfort Co., et al., v. International Registries, Inc., et al.*, 2015 WL 2238076, *10 n.10 (E.D. Va. 2015) (O'Grady, J.); *Plymouth Cnty. Retirement Ass'n. v. Primo Water Corp.*, 966 F. Supp. 2d 525, 536-37 (M.D.N.C. 2013).

II.   FACTUAL BACKGROUND

In an effort to stimulate the commercial space industry while leveraging those same commercial capabilities through public-private partnerships to deliver technologies and capabilities needed for future NASA and other governmental agency and commercial missions, NASA issued an RFP entitled "Utilizing Public-Private Partnerships to Advance Tipping Point Strategies." (Compl. ¶ 8).   Commonly referred to as "Tipping Point," this NASA program involves a variety of different smaller programs pursuing interesting but unrelated technologies. *(Id.*. ¶ 8-9, 48.) NASA awarded SSL a contract for its "Dragonfly" project in connection with this Tipping Point mission.   *(Id.* ¶ 10). NASA also awarded Orbital ATK a Tipping Point contract for its project named CIRAS.

In order for NASA to share information with the various contractors working with NASA on their respective Tipping Point projects – including Orbital ATK and SSL – NASA Langley Research Center ("NASA") set up a server identified as "NX." (Compl. ¶¶ 11, 15). On or about November 15, 2016, NASA granted access to an Orbital ATK employee working on its Tipping Point project. *(Id.* ¶ 11).   Once on the server, this employee was able to view information that went beyond just what was relevant to the CIRAS project. (*Id.*).   This apparently included documents SSL provided to NASA pertaining to SSL's unrelated Dragonfly project.   (*Id.* at 9-11) According to NASA's description of server activity, on or about November 23, 2016, this now-former employee opened and/or viewed four SSL-specific documents. (*Id.* ¶¶ 12-13).

Both NASA and Orbital ATK undertook investigations to ensure that no other copies of these documents existed anywhere on Orbital ATK's servers. (*Id.*; December 31, 2016 Letter

from S. Maclean to R. Flores, "Maclean Letter," attached hereto as Ex. 2).[2] According to SSL's

Complaint, about a week after Orbital ATK promptly self-reported the access to NASA, NASA

informed SSL. (Compl. ¶ 11). SSL then waited two weeks, until just before Christmas, on

December 19, 2016, to send Orbital ATK a letter seeking information about what had occurred.

(Compl. ¶ 15). Orbital ATK informed SSL that Orbital ATK had "taken the necessary action to

insure that no data was printed, copied or retained. All downloaded SSL data has been

destroyed; no current employees gleaned any knowledge or retained any information from the

disclosure; and the one employee whose actions violated [Orbital ATK's] ethics policy was

terminated." (Ex. 2, Maclean Letter; Compl. ¶ 19). Orbital ATK also confirmed that it had

cooperated fully with NASA regarding the issue, and was continuing to do so. (Ex. 2)

On December 31, 2016, Orbital ATK responded to SSL and made it clear that "no data

was printed, copied or retained," that "all downloaded SSL data has been destroyed," and that

"no current employees gleaned any knowledge or retained any information from the disclosure."

(Ex. 2, Maclean Letter). Further, Orbital ATK informed SSL that the employee who accessed

the information had been terminated, and assured SSL that Orbital ATK was "continuing to

communicate with NASA regarding their concerns." *Id.*

On February 7, 2017, Orbital ATK filed suit in this Court against DARPA. *See* DARPA

Complaint, Orbital ATK, Inc. and Space Logistics LLC v. Dr. Steven H. Walker, in his official

capacity as Acting Director of the DARPA, and the DARPA, 1:17-cv-00163-LMB-IDD

("DARPA Case"). Orbital ATK alleges that a contract awarded by DARPA to SSL violates the

---

[2] The Court can consider this letter at the motion to dismiss stage because it is referenced in the complaint. *Tellabs, Inc. v. Makor Issues & Rights, Ltd., et al.*, 551 U.S. 308, 322 (2007) ("[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice.")

National Space Policy. Specifically, Orbital ATK seeks judicial review under the Administrative

Procedures Act ("APA") of DARPA's decision to make the award as currently constituted to

SSL, under which "DARPA would pay to develop the robotic technology, pay to modify a

spacecraft platform, pay to launch the technology into orbit, and then (following a brief

demonstration period) transfer ownership of the significantly subsidized spacecraft – along with

the DARPA funded robotic technology – to SSL." (*See* DARPA Complaint, ¶ 4)

On March 22, 2017, just weeks after Orbital ATK filed the DARPA Case, SSL filed the

present suit, which alleged six counts and sought, *inter alia*, a preliminary injunction. The very

next day, SSL provided interviews to the press regarding their lawsuit, in which they made false

and unsupported allegations against Orbital ATK. (Ex. 1) Yet SSL has not moved for a

preliminary injunction. In fact, it did not even serve the Complaint on Orbital ATK for weeks,

and even then not until Orbital ATK's counsel contacted SSL to ask why it had filed this suit, but

withheld service in violation of this Court's local rules. L.R.Civ.P. 4(B) ("Requests by a party to

withhold the service of a summons and complaint … shall not be granted by the Clerk without

leave of Court first obtained….")

III.   LEGAL STANDARD

To survive a motion to dismiss under Rule 12(b)(6), SSL's "complaint must contain

sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face."

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (internal citation omitted). A claim is only facially

plausible if the plaintiff can offer "more than labels and conclusions" or "formulaic recitation of

the elements of a cause of action," and instead provides "grounds" of "entitle[ment] to relief."

Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007); *Craft v. Fairfax County Government*,

2016 WL 4140852, *4 (E.D. Va. 2016) (Cacheris, J.) (granting motion to dismiss under Rule

12(b)(6)). While the Court must view the complaint in the light most favorable to the plaintiff,

and take any well-pled factual allegations as true, this does not apply to "a legal conclusion couched as a factual allegation," *Papasan v. Allian*, 478 U.S. 265, 286 (1986); *Eastern Shore Markets, Inc. v. J.D. Associates Ltd. Partnership*, 213 F.3d 175, 180 (4th Cir. 2000); *Craft*, at *4, or to "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Veney v. Wyche*, 293 F.3d 726 (4th Cir. 2002).

ARGUMENT

I. SSL'S FEDERAL COMPUTER FRAUD AND ABUSE ACT CLAIM FAILS TO STATE A CLAIM

SSL's allegations under the Computer Fraud and Abuse Act, ("CFAA") 18 U.S.C. § 1030, *et seq.* amount to nothing more than a repetition of the elements of the statute and legal conclusions that SSL suffered harm. In fact, SSL does not even identify for the Court which provisions of the CFAA it alleges Orbital ATK supposedly violated, and for good reason: examining the statutory provisions reveals that SSL has not come close to pleading the elements of its claim. Plaintiff's CFAA count fails for multiple reasons. *First*, because SSL provided the information to NASA, who granted access to Orbital ATK, no claim under the CFAA can exist against Orbital ATK. *Second*, the requisite narrow construction of the statute, specifically what constitutes access "without authorization," mandates dismissal. *Finally*, Plaintiff offers no factual basis to even assert that it has suffered any damage as a result of the access. Each of these reasons alone is sufficient to grant Defendant's motion to dismiss.

A. NASA Granted Orbital ATK Access to Its Server and Thus There Can Be No Claim Against Orbital ATK As a Matter of Law

This Court has held that when an owner of information (here SSL) provides it to the owner of the Protected Computer (NASA), and the computer's owner provides access to a third party (Orbital ATK), there cannot be a claim under the CFAA against the third party (Orbital ATK). Two cases from this Court confirm that SSL cannot assert a CFAA claim against Orbital

6

ATK. First, in *State Analysis, Inc. v. American Financial Services Assoc.*, the plaintiff, StateScape, created and operated a proprietary database of bills, regulations, and the analysis of both. 621 F. Supp. 2d 309, 316-17 (E.D. Va. 2009) (Brinkema, J.). StateScape had granted access, through log-ins and passwords, to Defendant American Financial Services Association ("AFSA"), and Kimbell Sherman Ellis ("KSE"), a government relations firm who had been a customer of StateScape for a brief 11-month period, but then became a competitor. *Id.* at 313-14. Plaintiff asserted a CFAA violation against both AFSA and KSE based on the allegations that AFSA provided its passwords to StateScape's database to KSE, allowing KSE to access, download, and misappropriate StateScape's copyrighted information. *Id* The Court dismissed the CFAA claim against AFSA. Recognizing that "some authorities have held that the CFAA was targeted at 'computer hackers' Judge Brinkema held that the statute "only applies to a situation where an outsider, or someone without authorization, accesses a computer." *Id. at 315-16* (internal citations omitted).

Second, in *SecureInfo Corp. v. Telos Corp.,* the plaintiff entered into a consulting agreement with defendant Berman and, as part of that relationship, provided its software to Berman. 387 F. Supp. 2d 593, 609 (E.D. Va. 2005) (Lee, J.). Defendant Berman then gave access to plaintiff's software to employees of defendants Telos and Xacta, competitors of the plaintiff. *Id.* The plaintiff brought several claims, including CFAA claims against Berman, Telos, and Xacta. Telos and Xacta moved to dismiss the CFAA claims against them, arguing that because the plaintiff allowed Berman to store plaintiff's information, any access by Telos or Xacta could not be "unauthorized" under the CFAA as a matter of law. The Court agreed, holding that "even if Mr. Berman allowed the defendants access to the BAI server and SecureInfo's materials *in violation of the license agreements*, under his grant of authority to the

7

defendants, they were entitled to obtain the information on the server." *Id.* at 609 (emphasis added).

SSL admits that it provided its documents relating to the Dragonfly project to NASA. (Compl. ¶¶ 9, 10, 50). NASA, the owner of the Protected Computer at issue here, put this information on its NX server. NASA then granted Orbital ATK's employee access to the NX server. Therefore, any access by Orbital ATK's employee to the NX server cannot be unauthorized as a matter of law as *State Analysis* and *SecureInfo* hold. Other cases are in accord. *Lockheed Martin Corp. v. Speed, et al.*, 2006 WL 2683058 (Aug. 1, 2006) (granting motion to dismiss CFAA claim, finding that employees who were authorized to access computer could not violate statute even when they removed trade secret and provided it to a competitor). *See also AtPac, Inc. v. Aptitutde Solutions, Inc.*, 730 F. Supp. 2d 1174 (E.D. Cal. 2010).

B. The Narrow Construction of the CFAA Also Forecloses SSL's Claims

Courts narrowly construe the private cause of action available under the CFAA, which was originally a criminal statute enacted to combat malicious hacking of computer systems. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012) ("Today, the CFAA remains primarily a criminal statute designed to combat hacking.") Courts are clear that the later-added civil remedy must be interpreted narrowly. *U.S. v. Santos,* 553 U.S. 507, 541 (2008); *WEC Carolina*, 687 F.3d at 203 ("Where, as here, our analysis involves a statute whose provisions have both civil and criminal application, our task merits special attention because our interpretation applies uniformly in both contexts. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n. 8 (2004). Thus, we follow 'the cannon of strict construction of criminal statutes, or rule of lenity.'") Further, as the statutory language makes clear, subsections 1030(a)(5)(B) and (C) –

which appear to be the sections SSL alleges were violated[3] – do not apply to permitted users. Specifically, these provisions of the CFAA state that, "[w]hoever intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." 18 U.S.C. 1030(a)(5)(B) and (C). They "are intended to apply to outsiders who access a computer," not to insiders who access computers with the owner's permission. *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F. Supp. 2d 1359, 1370-71 (S.D. Fla. 2001). Because here there is no dispute that the Orbital ATK employee properly had access to the NASA server, no claim under the CFAA is possible.

Even if SSL is seeking relief under a different provision of the statute, the narrow construction necessarily applicable to the CFAA would bar such a claim. Under the narrow construction courts apply to the CFAA, the term "exceeds authorized access" means "to access a computer ***without authorization***" and to use such access to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter." 18 U.S.C. § 1030(e)(6). As explained above, this provision is construed narrowly. *AtPac, Inc.,* 730 F. Supp. 2d at 1180. In *AtPac*, Plaintiff AtPac was the system administrator for Defendant Nevada County's ER-Recorder server. *Id.* at 1176. The server was segregated into two sets of directories; one, to which Nevada County and its employees had password-protected access, that stored the customer data, and one that contained AtPac's proprietary source code, which Nevada County's employees did not have access to. *Id.* AtPac restricted access to its source code directories to itself and Nevada County for the sole purpose of powering down the server in the event of an

---

[3] SSL does not cite or refer to any specific provision of the CFAA, leaving Orbital ATK to speculate under which provision(s) SSL is seeking relief. (Compl. ¶¶ 70-81)

emergency. *Id.* at 1177. AtPac alleged that the county used its emergency-only password to provide access to AtPac's source code to Aptitude, which was replacing AtPac as the software provider in violation of multiple provisions of the CFAA, including §§ 1030(a)(2)(c), and (a)(4)-(6). *Id.* at 1178. The Court found that "the rule of lenity required the term 'authority' be construed such that employees did not automatically lose 'authority' to access a computer when they violate their duty of loyalty to their employer by accessing the computer with an improper purpose." *Id.* at 1180. In granting Defendants' motion to dismiss, the Court held, "[s]imply put, a person cannot access a computer 'without authorization' if the gatekeeper has given them permission to use it." *Id.* SSL's complaint itself admits that the Orbital ATK employee ***was authorized*** to access the NASA NX server as part of Orbital ATK's work for NASA on the CIRAS Tipping Point project. (Compl. ¶ 11). This simple fact is sufficient to defeat SSL's claim.

C. Plaintiff Cannot Sufficiently Plead "Damage" As Required by the CFAA

To adequately allege a claim under the CFAA, SSL must sufficiently plead either damage (18 U.S.C. § 1030(a)(5)(B)) or damage and loss (18 U.S.C. § 1030(a)(5)(C).) Because SSL fails to allege facts sufficient to establish it has suffered any damage, its CFAA claim fails for this independent reason. Under the CFAA, "damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information" 18 U.S.C. § 1030(e)(11). SSL's allegations regarding its supposed damages are wholly insufficient.

SSL's complaint is utterly devoid of any allegation that the integrity or availability of its documents has been impaired in any way. *Id.* SSL does not claim that its information has been used, altered or removed from the server. It has been months since the November 2016 incident occurred on NASA's NX server, and SSL's complaint lacks any reference, evidence or even an

indication that the information contained in these documents has been used. SSL's claim of damages relates solely to the alleged loss of trade secrets, but courts have found that this alone is not sufficient to establish damages under the CFAA. *Lockheed Martin*, 2006 WL 2683058, at *3. In *Lockheed*, the company alleged that its employees conspired with a competitor to provide copies of Lockheed's trade secrets in order to assist the competitor in responding to an RFP issued by the Air Force. *Id.* at *1. The Court found that even alleging the "wrongful taking of trade secrets does not, by itself, fit within the grouping of "damage" or "loss." *Id.* at *3 (citing *Resdev, LLC v. Lot Builders Ass'n, Inc.*, 2005 WL 1924743, *4 (M.D. Fla. Aug. 10, 2005).

SSL's damages allegations amount to nothing more than that the documents have been accessed and copied by Orbital ATK. (Compl. ¶ 57). This is also insufficient under the CFAA because "***the mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement***." *Farmers Ins. Exchange v. Auto Club Group*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011) (citations omitted). In *Farmers*, Plaintiff Farmers Insurance Exchange alleges that some of its independent contractor agents accessed its proprietary database, the Agency Dashboard, and provided that information to Defendant Auto Club Group. However, Auto Club points out that "Farmers has not alleged 'any diminution in the completeness or usability of the Agency Dashboard … [or] that [Auto Club's] actions resulted in lost or corrupted data, the unavailability of the Agency Dashboard to other users, or any physical damage to [Farmers'] servers.'" *Id.* at 853. The Court agreed with Auto Club that "Farmers has neither pleaded nor argued that Auto Club actually impaired its databases or data…." *Id.*

SSL's complaint fails to establish several critical elements of a CFAA claim, including unauthorized access, as well as damage. For the reasons stated above, SSL's CFAA claim must be dismissed.

II.   SSL'S TRADE SECRET CLAIMS ARE INADEQUATELY PLED AND FAIL AS A MATTER OF LAW.

SSL's state and federal law trade secret claims require substantially the same elements to be pled, and suffer from the same defects requiring their dismissal. Virginia's version of the Uniform Trade Secrets Act ("VUTSA"), Va. Code § 59.1-336, requires a plaintiff to establish that (1) the information in question constitutes a trade secret, and (2) the defendant misappropriated it. *E. W., LLC v. Rahman,* 873 F. Supp. 2d 721, 735–36 (E.D. Va. 2012) (Cacheris,   J.)   (dismissing   VUTSA   claim   as   inadequately   pled)   (citing *MicroStrategy, Inc. v. Bus. Objects, S.A.,* 331 F. Supp.2d 396, 416 (E.D. Va. 2004) (Friedman, J.)). The VUTSA defines misappropriation as:

> 1. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was ***acquired by improper means***; or
>
> 2. ***Disclosure or use*** of a trade secret of another without express or implied consent by a person who
>
>> a.   Used improper means to acquire knowledge of the trade secret; or
>>
>> b.   At the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was
>>
>>> (1) Derived from or through a person who had utilized improper means to acquire it;
>>> (2) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use;
>>> (3) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>>> (4) Acquired by accident or mistake.

Va. Code § 59.1-336 (emphasis added). *See also Softech Worldwide, LLC v. Internet Tech. Broadcasting Corp.,* No. 1:10cv651, 2010 WL 4645791, at *5 (E.D. Va. Nov. 8, 2010) (Cacheris, J.) (dismissing VUTSA claim as inadequately pled).

The federal Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1832, *et seq*., includes definitions, remedies, and a statute of limitations substantially similar to provisions in the

Uniform Trade Secrets Act ("UTSA"); H. Rep. No. 114-529, at 4-5, 12-14 (2016), as reprinted in 2016 U.S.C.C.A.N. 195-211. In relevant part, the DTSA defines trade secret misappropriation as one where the defendant:

> with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--
> (**1**) steals, or without authorization appropriates, takes, carries away, or conceals, or *by fraud, artifice, or deception* obtains such information;
> (**2**) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
> (**3**) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted *without authorization*;
> (**4**) attempts to commit any offense described in paragraphs (1) through (3); or
> (**5**) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy.

18 U.S.C. § 1832(a) (emphasis added). Thus, in order to make out a claim under the DTSA, a plaintiff must show "an unconsented disclosure or use of a trade secret by one who (i) used improper means to acquire the secret, or, (ii) at the time of disclosure, knew or had reason to know that the trade secret was acquired through improper means, under circumstances giving rise to a duty to maintain the secrecy of the trade secret, or derived from or through a person who owed such a duty." *Free Country Ltd v. Drennen*, No. 16 CV 8746 (JSR), 2016 WL 7635516, at *3 (S.D.N.Y. Dec. 30, 2016) (citation omitted).

    A.   **SSL Fails To Plead Adequately That Its Information Constituted Trade Secrets.**

To establish that something is deserving of the label 'trade secret,' "the information must be of a subject matter entitled to trade secret protection, must have independent economic value as a result of not being generally known and not being readily ascertainable by proper means; and reasonable efforts must have been taken to maintain its secrecy." *MicroStrategy*, 331 F.

Supp. 2d at 416. At the pleading stage, SSL was required to plead more than simply "conclusory allegations" that its information amounted to supposed trade secrets; it needed to plead "factual allegations to support this assertion." *E. W., LLC,* 873 F. Supp. 2d at 735–36 (citing *All Bus. Solutions, Inc. v. NationsLine, Inc.,* 629 F.Supp.2d 553, 558–59 (W.D. Va. 2009) (Conrad, J.) (dismissing VUTSA claim consisting of conclusory allegations that the defendant misappropriated customer names, along with other trade secrets and confidential information, and which lacked supporting factual allegations)); *Softech Worldwide,* LLC, 2010 WL 4645791, at *5.

In its Complaint, however, SSL provides nothing more than a laundry list of the categories of allegedly proprietary information contained in the documents it believes were accessed by the now-former Orbital ATK employee. (Compl. ¶ 59). But SSL's conclusory statements are not sufficient to establish that the documents are entitled to trade secret protection. *E. W., LLC,* 873 F. Supp. 2d at 735–36; *All Bus. Solutions, Inc.,* 629 F. Supp. 2d at 558–59; *Softech Worldwide,* LLC, 2010 WL 4645791, at *5. While, as a general matter, these types of information may be entitled to trade secret status, SSL does not plead *facts* – as opposed to legal labels – about the actual information contained in the documents, their independent economic value, and their unascertainable nature. To the contrary, what SSL actually pleads, as well as the context of its claims, confirms that SSL does not allege facts sufficient to support its DTSA claim. According to SSL, only two of the documents were even marked "SSL Proprietary," and all four documents were shared with NASA. (Compl. ¶¶ 62, 65). SSL waited three months after learning about the access to even file this complaint. SSL then withheld service of its complaint for weeks after filing (without leave of court as required by the local rules) until after Defendant's counsel contacted SSL's lawyers to seek an explanation for the surprising, and

14

meritless, filing.   L.R.Civ.P. 4(B). Finally, while in the Complaint SSL supposedly asks this

Court for a preliminary injunction, it has taken no steps to actually seek such relief, implicitly

recognizing the weakness of its claims. Taken together, these facts drastically undermine SSL's

claim that these documents are protected trade secrets. SSL does not allege adequately that the

documents were trade secrets, and thus fails to plead a plausible entitlement to relief. *Twombly*,

550 U.S. at 555.

B.   **SSL Fails To Plead Misappropriation Plausibly**

The VUTSA and DTSA provide two methods by which misappropriation can be

accomplished, but SSL does not allege facts that would amount to either.   The first requires

"acquisition of a trade secret of another by a person who knows or has reason to know that the

trade secret was acquired by improper means." Va. Code § 59.1-336; *see also* 18 U.S.C. § 1832

(a)(1)-(3). But SSL offers no facts sufficient to demonstrate that the now-former Orbital ATK

employee encountered any obstacles or other warnings when accessing NASA's NX server that

he was not permitted to view these documents. The mere labeling of documents as "proprietary"

is not enough, especially in the government contracts context involving proposal documents.

MicroStrategy, 331 F. Supp. 2d at 427 ("Although it was marked confidential, this fact alone is

not dispositive and does not raise a document to the status of trade secret in the absence of other

evidence."); *see also Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1333 (N.D.

Ga. 2007) ("Thus, where the plaintiff has distributed to its customers schematic diagrams, repair

instructions, product manuals, or similar information – even if they are labeled "proprietary" or

"confidential" – the plaintiff's failure to maintain secrecy precludes trade secret protection.")

Therefore, SSL's assertion that two of the documents were marked proprietary is not sufficient to

establish knowledge on the part of the employee. This is to say nothing of the two documents

that SSL admits were not so marked and gave no indication that they were allegedly proprietary.

Even if the materials accessed were trade secrets, if no improper means were used to

obtain the trade secrets, *i.e.*, it was obtained by accident or mistake, then SSL must plead with

plausible facts (not labels) that the trade secrets were disclosed or used, the second method of

misappropriation. *MicroStrategy*, 331 F. Supp. 2d at 417. The second method of achieving

misappropriation requires the "disclosure or use of a trade secret of another without express or

implied consent…." Va. Code § 59.1-336; *see also* § 1832 (a)(1)-(3). SSL does not allege more

than conclusory labels that the information contained in the accessed documents has been used or

disclosed in any way by Orbital ATK. (Compl. ¶ 88.c ("Upon information and belief, using and

disclosing the Confidential Information identified herein for the benefit of Orbital ATK.").

Thus, as in *E.W.*, SSL "fails to allege how [Orbital ATK] used this information or that

they did so knowing that the information was confidential." *E. W., LLC,* 873 F. Supp. 2d at 735–

36 (citing *Softech,* 2010 WL 4645791, at *5 (emphasizing that misappropriation "includes

a *knowledge* element") (emphasis in original)). "Because 'naked assertion[s]' devoid of 'further

factual enhancement' are insufficient to withstand a motion to dismiss," SSL's trade secret

counts both fail to state a claim. *Id.* (citing *Iqbal v. Ashcroft,* 556 U.S. 662, 678 (2009)

(quoting *Twombly,* 550 U.S. at 557).[4]

---

[4] If Plaintiff's federal claims are dismissed, as they should be, this Court loses jurisdiction as the
Plaintiff's sole pled basis for jurisdiction is federal question jurisdiction. (Compl. ¶ 27; 28 U.S.
Code § 1331.)

III. **SSL'S REMAINING STATE LAW CLAIMS FAIL AS A MATTER OF LAW BECAUSE THEY ARE INADEQUATELY PLED OR PREEMPTED BY STATUTE**

A. **Plaintiff Fails to State a Claim for a Violation of the Virginia Computer Crimes Act Because the Access Was Not Unauthorized**

SSL's claim under the Virginia Computer Crimes Act fails because, as with its CFAA claim, SSL's facts do not establish that the Orbital ATK employee was not authorized to access the NASA NX server. A violation of the VCCA requires that a party "(1) uses a computer or computer network; (2) *without authority*; and (3) either obtains property or services by false pretenses, embezzles or commits larceny, or converts the property of another." Va. Code § 18.2-152.3, *et seq.* (emphasis added); *In re Hackman*, 534 B.R. 867, 879 (E.D. Va. Bkrtcy Ct. 2015) (Court dismissed CVVA claim for failure to state a claim because "[i]t is the ***unauthorized use*** of a computer network that gives rise to liability under the VCCA, not the authorized use of a computer network for the receipt of arguably illicit funds.") (emphasis added); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 934 (E.D. Va. 2010) (Brinkema, J.) (granting motion to dismiss VCCA claim).

As detailed above, because SSL fully admits that the Orbital ATK employee had the authority to access NASA's NX server, SSL cannot make out a claim under the VCCA. In *Supinger v. Virginia*, plaintiff alleged that "Defendants 'used a computer or computer network to intentionally examine without authority Supinger's identifying information …." 167 F. Supp. 3d 795, 821 (W.D. Va. 2016) (Moon, J.). The Court dismissed plaintiff's VCCA claim because there was no support for the contention that Defendants acted "without authority." *Id.* Similarly, here SSL alleges that "Orbital ATK intentionally used NASA's NX server system, without authorization or exceeding authorized access, to make or cause to be made an unauthorized copy

of information…." (Compl. ¶ 103). SSL's allegation provides no more specificity than the

plaintiff in *Supinger*; thus its Complaint should suffer the same consequences.

Further, SSL offers no facts to support a claim that it was harmed in any way by the

employee's actions. The conclusory statement that "Orbital ATK substantially injured SSL by

improperly obtaining SSL's valuable and confidential proprietary information and trade secrets,

and using them for purposes not authorized by SSL" (Compl. ¶ 104) does not "raise a right to

relief above the speculative level." *Stultz v. Va. Dep't. of Motor Vehicles, et al.*, 185 F. Supp. 3d

890, 903-04 (W.D. Va. 2015) (Conrad, J.) (dismissing plaintiff's claim of violation of Va. Code

§ 18.2-152.5). There is no attempt to describe what, if any, purpose Orbital ATK supposedly

used these documents for, let alone how SSL was actually, not potentially, harmed.

B. Plaintiff's Conversion Claim Is Preempted and – Even if it Were Permitted – Not Plausibly Pleaded

Plaintiff's claim for conversion must be dismissed because it is preempted by its claim

under the Virginia Uniform Trade Secrets Act. As the Court held in *E.I. DuPont de Nemours*

and Co. v. Kolon Industries, Inc., when a conversion claim is based entirely on the alleged

misappropriation of trade secrets, as it is here, it is preempted by the VUTSA. 688 F. Supp. 2d

443, 450 (E.D. Va. 2009) (Payne, J.); Va. Code § 59.1-341. A review of SSL's allegations under

Count V makes it clear that its conversion claim relates solely and entirely to the supposed

misappropriation of SSL's documents. Therefore, this claim is preempted by the VUTSA and

must be dismissed.

Independently, other than the conclusory repetition of the elements of a conversion claim,

SSL provides no facts supporting the claim that one Orbital ATK ex-employee's transient access

to the documents impeded or interfered with SSL's ability to utilize the documents, or was in any

way inconsistent with SSL's rights to the documents. Instead, SSL uses this claim to further its

agenda of defaming Orbital ATK by alleging, without any good faith basis to do so, that the so-called conversion was "in support of Orbital ATK's general strategy to eliminate and/or hinder SSL from competing in the robotic satellite servicing arena." (Compl. ¶ 110). Although it provides no support for SSL's claims, this statement does reveal the improper motive behind this suit.

C. Plaintiff's Claim for Unjust Enrichment Is Preempted As Well.

Just as with its claim for conversion, SSL's claim for unjust enrichment is also preempted by the Virginia Uniform Trade Secrets Act. As explained in *E.I. DuPont*, the VUTSA preempts all claims for relief, including common law claims, if they provide a civil remedy for misappropriation of trade secrets. As above, SSL's claim for unjust enrichment is based entirely on the alleged misappropriation and is therefore preempted and must be dismissed. 688 F. Supp. 2d 443, 450 (E.D. Va. 2009); Va. Code § 59.1-341.

CONCLUSION

For the reasons stated above, SSL's complaint is wholly insufficient, fails to state a claim for which relief may be granted, and must be dismissed in its entirety.

Dated: June 23, 2017   ORBITAL ATK, INC.

By Counsel:

/s/ Billy B. Ruhling, II
Bernard J. DiMuro, Esq. (VSB #187784)
Billy B. Ruhling, II, Esq. (VSB #45822)
DIMUROGINSBERG, P.C.
1101 King Street, Suite 610
Alexandria, Virginia 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Emails: bdimuro@dimuro.com
         bruhling@dimuro.com

Rebecca R. Anzidei (VSB #46436)
Philip J. O'Beirne (VSB #71956)
STEIN MITCHELL CIPOLLONE BEATO & MISSNER LLP
1100 Connecticut Avenue, NW Suite 1100
Washington, D.C. 20036
Telephone: (202) 737-7777
Facsimile: (202) 296-8312
Email: ranzidei@steinmitchell.com
        pobeirne@steinmitchell.com

CERTIFICATE OF SERVICE

I hereby certify that on the 23rd day of June, 2017, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send notice of such filing to counsel of record that are registered with CM/ECF.

                    /s/
                    Billy B. Ruhling, II